Defense Information Systems Agency
Joint Information & Engineering Organization
Center for Information Technology Standards
http://www-pki.itsi.disa.mil/

8 MAY 2000

DRAFT Online Certificate Status Protocol (OCSP) Profile - **DRAFT**

Reference:

RFC 2279	UTF-8, a transformation format of ISO 10646
RFC 2437	PKCS #1: RSA Cryptography Specifications, Version 2.0
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
X.509	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
FIPS 180-1	Secure Hash Standards, 17 April 1995
DoD SPEC	Department of Defense Class 3 Pulic Key Infrastructure Interface Specification, 13 Januray 2000 (DRAFT)

Protocol

Protocol Action	**Status**	**Notes**
OCSP Server		
CAs shall include the AuthorityInfoAccess extension in certificates that are to be checked using OCSP.	M	[RFC 2459: 4.2.2.1] [RFC 2560: 3.1]
CAs that support an OCSP service must provide for the inclusion of a value for a uniformResourceIndicator (URI) accessLocation and the OID value id-ad-ocsp for the accessMethod in the AccessDescription SEQUENCE.	M	[RFC 2560: 3.1]
The value of the accessLocation field in the subject certificate defines the transport (e.g. HTTP) used to access the OCSP responder.	M	[RFC 2560: 3.1]
The value of the accessLocation field in the subject certificate may contain other transport dependent information (e.g. a URL).	I	[RFC 2560: 3.1, DoD SPEC: 5] URLs for Chambersburg, Denver and other replicated sites.
The delegated OCSP responder's signing certificate shall include id-kp-OCSPSigning in an extendedKeyUsage certificate extension.	M	id-kp-OCSPSigning OID ::= {id-kp 9} [RFC 2560: 4.2.2.2]

Protocol Action	Status	Notes
A CA may specify a responder can be trusted for the lifetime of the responder's certificate.	I	[RFC 2560: 4.2.2.2.1, DoD SPEC: 5]
The extension id-pkix-ocsp-nocheck is included in the responder's certificate.	m	id-pkix-ocsp-nocheck OID ::= {id-pkix-ocsp 5} [RFC 2560: 4.2.2.2.1]
This should be a non-critical extension.	I	[RFC 2560: 4.2.2.2.1]
The value of the extension should be NULL.	I	[RFC 2560: 4.2.2.2.1]
CAs may issue this certificate with a very short lifetime and renew it frequently.	I	A compromise of the responder's key is as serious as the compromise of a CA key used to sign CRLs. Seems to be the safest thing to do. [RFC 2560: 4.2.2.2.1]
A CA may specify how the responder's certificate is checked for revocation.	I	[RFC 2560: 4.2.2.2.1]
CRL Distribution Points can be provided if the check should be done using CRLs or CRL Distribution Points.	I	[RFC 2459: 4.2.1.14; RFC 2560: 4.2.2.2.1]
Authority Information Access can be provided to access CA on-line validation services (excluding CRLs).	No	[RFC 2459: 4.2.2.1; RFC 2560: 4.2.2.2.1] Private extension.
A CA may choose not to specify any method of revocation checking for the responder's certificate.	NO	[RFC 2560: 4.2.2.2.1]

OCSP Client		
Systems or applications that rely on OCSP responses must be capable of detecting and enforcing use of the id-ad-ocspSigning value.	M	[RFC 2560: 4.2.2.2]
Applications that receive certificates with other transport dependent information contained in the accessLocation field must be able to process this infromation	M	
At the OCSP client, the accessLocation for the one or more OCSP signing authorities may be configured, and the set of CAs for which each signing authority is trusted specifed.	I	[RFC 2560: 3.1, 4.2.2.2, DoD SPEC: 5]
Prior to accepting a signed response as valid, OCSP clients shall confirm that: 1. The certificate identified in a received response corresponds to that which was requested 2. The signature on the response is valid 3. The identity of the signer matches the intended recipient of the request 4. The signer is currently authorized to sign the response 5. The time at which the status being indicated is known to be correct (thisUpdate) is sufficiently recent 6. When provided, the time at or before which newer information will be available about the status of the certificate (nextUpdate) is greater than the current time	M	[RFC 2560: 3.2]

Protocol Action	Status	Notes
If the certificate validating the signature on the response fails to meet at least one of the following criteria, the confirmation that the signer is authorized to sign fails and the response is rejected: 1. Matches a local configuration of OCSP signing authority for the certificate in question; or 2. Is the certificate of the CA that issued the certificate in question; or 3. Includes a value of id-ad-ocspSigning in an ExtendedKeyUsage extension and is issued by the CA that issued the certificate in question."	M	[RFC 2560: 4.2.2.2]
The client may apply additional acceptance or rejection criteria either to the response or to the certificate used to validate the signature on the response.	NO	[RFC 2560: 4.2.2.2]
If an internalError error message is returned, the OCSP requestor should retry, potentially with another OCSP responder.	I	[RFC 2560: 2.3]
OCSP clients shall be capable of receiving and processing responses of the id-pkix-ocsp-basic response type.	M	[RFC 2560: 2.2, 4.2.1, 4.4.3]
The client is to interpret the thisUpdate and nextUpdate fields as defining a recommended validity interval.	M	[RFC 2560: 4.2.2.1]
Responses whose nextUpdate value is earlier than the local system time value should be considered unreliable.	I	[RFC 2560: 4.2.2.1]
Responses whose thisUpdate time is later than the local system time should be considered unreliable.	I	[RFC 2560: 4.2.2.1]
OCSP clients must check that an authorized responder's certificate has not been revoked.	M	[RFC 2560: 4.2.2.2.1]
Applications that receive certificates indicating that the responder should be trusted for the responder's certificate lifetime must be able process the certificate according to local policy.	M	
If the responder's certificate includes the extension id-pkix-ocsp-nocheck an OCSP client may trust a responder for the lifetime of the certificate.	I	[RFC 2560: 4.2.2.2.1, DoD SPEC: 5]
The OCSP client must indicate its support by including the id-pkix-ocsp-nocheck OID in the AcceptableResponses SEQUENCE.	m	[RFC 2560: 4.4.3]
Applications that receive certificates specifying how the responder's certificate is checked for revocation must be able to use the revocation method specified.	M	
If the CA does not specify any method of revocation checking for the responder's certificate, the OCSP client must follow it's local security policy on whether that certificate should be checked for revocation.	M	[RFC 2560: 4.2.2.2.1]
Clients shall be capable of processing responses signed using DSA keys identified by the DSA sig-alg-oid.	M	[RFC2459: 7.2.2; RFC 2560: 4.3]
Clients should also be capable of processing RSA signatures.	I	[RFC2459: 7.2.1; RFC 2560: 4.3]

Protocol Action	Status	Notes
The OCSP client may indicate its support of nonce cryptographic binding a request and a response by including OID id-pkix-ocsp-nonce OID in the AcceptableResponses SEQUENCE, while the extnValue is the value of the nonce.	NO	id-pkix-ocsp-nonce OID ::= { id-pkix-ocsp 2 } [RFC 2560: 4.4.1]
The OCSP client may indicate its support for CRL references by including the id-pkix-ocsp-crl OID in the AcceptableResponses SEQUENCE.	I	[RFC 2560: 4.4.2]
OCSP client MAY wish to specify the kinds of response types it understands.	I	[RFC 2560: 4.4.3]
OCSP client SHOULD use an extension with the OID id-pkix-ocsp-response, and the value AcceptableResponses.	I	The OIDs included in AcceptableResponses are the OIDs of the various response types this client can accept. id-pkix-ocsp-response OID ::= { id-pkix-ocsp 4 } [RFC 2560: 4.4.3]
This extension is included as one of the requestExtensions in requests.	m	[RFC 2560: 4.4.3]
An OCSP archive cutoff date is used to prove digital signature reliability as of the date it was produced. Even if the certificate validating the signature has expired.	M	[RFC 2560: 4.4.4]

OCSP Request

An OCSP request will contain: 1. protocol version 2. service request 3. target certificate identifier	M	Requests do not contain the responder they are directed to. This allows an attacker to replay a request to any number of OCSP responders. [RFC 2560: 2.1, 5, DoD SPEC: 5]
An OCSP request may contain optional extensions.	I	[RFC 2560: 2.1, 4.1.2, DoD SPEC: 5]
The critical flag should not be set for any of them.	I	[RFC 2560: 4.1.2]
The requestor may choose to sign the OCSP request.	NO	[RFC 2560: 4.1.2, DoD SPEC: 5]
For signature calculation, the data to be signed is encoded using the ASN.1] distinguished encoding rules (DER) [X.690].	m	[RFC 2560: 4]
The signature is computed over the tbsRequest structure.	m	[RFC 2560: 4.1.2]
The requestor shall specify its name in the requestorName field.	m	[RFC 2560: 4.1.2]
The requestor may include certificates that help the OCSP responder verify the requestor's signature in the certs field of Signature.	No	[RFC 2560: 4.1.2]
Formatting of the request message could vary depending on the transport mechanism used (HTTP, SMTP, LDAP, etc.).	I	[RFC 2560: 4.1, 5]
The request message is formatted for HTTP.	I	Implementers are advised to consider the reliability of HTTP cache mechanisms when deploying OCSP over HTTP. [RFC 2560: 4.1, 5, DoD SPEC: 5]
The request message is formatted for SMTP.	No	[RFC 2560: 4.1, 5]

Protocol Action	Status	Notes
The request message is formatted for LDAP.	I	[RFC 2560: 4.1, 5]
The serviceLocator request extension may be included as one of the singleRequestExtensions in requests.	I	id-pkix-ocsp-service-locator OID ::= { id-pkix-ocsp 7 } [RFC 2560: 4.4.6]
Values for the issuer and locator fields are obtained from the corresponding fields in the subject certificate.	m	[RFC 2560: 4.4.6]

OCSP Responder

Upon receipt of request the OCSP Responder determines if: 1. the message is well formed 2. the responder can provide requested service 3. the request contains the needed information	M	[RFC 2560: 2.1]
If one of the conditions is not meet, the OCSP Responder returns an error message.	M	[RFC 2560: 2.1, 2.3]
If the conditions are met, the OCSP Responder returns a message containing requested service.	M	[RFC 2560: 2.1]
Upon receipt of request, the OCSP Responder may process requested extensions.	I	[RFC 2560: 2.1]
Unrecognized, non-critical extensions must be ignored	m	[RFC 2560: 4.1.2]
Unrecognized, critical extensions must be handled by an exception routine.	m	[RFC 2560: 4.1.2]
The key used to sign the response must belong to one of the following:	M	[RFC 2560: 2.2, 4.2.2.2]
The CA who issued the certificate in question	No	[RFC 2560: 2.2]
A Trusted Responder whose public key is trusted by the requester	I	[RFC 2560: 2.2, DoD SPEC: 5]
A CA Designated Responder (Authorized Responder)	No	[RFC 2560: 2.2]
OCSP responders shall be capable of producing responses of the id-pkix-ocsp-basic response type.	M	[RFC 2560: 2.2, 4.2.1, 4.4.3]
OCSP responders may pre-produce signed responses specifying the status of certificates at a specified time.	NO	The use of pre-produce responses allows replay attacks. [RFC 2560: 2.5, 5]
The time at which the status was known to be correct shall be reflected in the thisUpdate field of the response.	NO:m	[RFC 2560: 2.5]
The time at or before which newer information will be available is reflected in the nextUpdate field.	NO:m	[RFC 2560: 2.5]
The time at which the response was produced will appear in the producedAt field of the response.	NO:m	[RFC 2560: 2.5]
A certificate's issuer may delegate OCSP signing authority.	I	[RFC 2560: 2.6, DoD SPEC: 5]
An Authorized OCSP Responder must have a certificate containing a unique value for extendedKeyUsage.	m	id-kp-OCSPSigning OID ::= {id-kp 9} [RFC 2560: 2.6, 4.2.2.2, RFC 2459: 4.2.1.13]
An Authorized Responder must receive this certificate directly from the delegating CA.	m	[RFC 2560: 2.6]

Protocol Action	Status	Notes
If an OCSP responder knows that a particular CA's private key has been compromised, it MAY return the revoked state for all certificates issued by that CA.	I	[RFC 2560: 2.7]
An Authorized OCSP responder may provide status information for one or more CAs.	I	[RFC 2560: 4.2.2.2.1]
OCSP responders shall support the SHA1 hashing algorithm.	M	[RFC 2560: 4.3]
The OCSP responder may support nonce cryptographic binding a request and a response by including OID id-pkix-ocsp-nonce as one of the responseExtensions.	NO	id-pkix-ocsp-nonce OID ::= { id-pkix-ocsp 2 } [RFC 2560: 4.4.1]
The OCSP responder may indicate the CRL on which a revoked or onHold certificate is found.	I	[RFC 2560: 4.4.2]
The CRL may be specified by a URL where it is available.	I	[RFC 2560: 4.4.2]
The CRL may be specified by its CRL number.	No	[RFC 2560: 4.4.2]
The CRL may be specified by the time at which the relevant CRL was created.	No	[RFC 2560: 4.4.2]
These extensions will be specified as response singleExtensions.	m	[RFC 2560: 4.4.2]
The identifier for this extension will be id-pkix-ocsp-crl, while the value will be CrlID.	m	id-pkix-ocsp-crl OID ::= { id-pkix-ocsp 3 } [RFC 2560: 4.4.2]
An OCSP responder may choose to retain revocation information beyond a certificate's expiration.	I	[RFC 2560: 4.4.4]
The archive cutoff date is determined by subtracting the retention interval value from the producedAt time.	m	[RFC 2560: 4.4.4]
In order to support such historical reference an archive cutoff date extension should be included in responses.	I	[RFC 2560: 4.4.4]
If included, this value shall be provided as an OCSP singleExtensions extension identified by id-pkix-ocsp-archive-cutoff and of syntax GeneralizedTime.	m	id-pkix-ocsp-archive-cutoff OID ::= { id-pkix-ocsp 6 } [RFC 2560: 4.4.4]
An OCSP server may upon receiving a request route it to the OCSP server, which is known to be authoritative for the identified certificate.	M	[RFC 2560: 4.4.6]

OCSP Response		
OCSP response consists of response type and data.	M	[RFC 2560: 2.2]
All non-error response messages must be digitally signed.	M	[RFC 2560: 2.2]
A response message is composed of: 1. version of the response syntax 2. name of the responder 3. responses for each of the certificates in a request 4. optional extensions 5. signature algorithm OID 6. signature computed across hash of the response	M	[RFC 2560: 2.2, DoD SPEC: 5]

Protocol Action	Status	Notes
The response for each of the certificates in a request consists of: 1. target certificate identifier 2. certificate status value 3. response validity interval	M	[RFC 2560: 2.2, DoD SPEC: 5]
The response for each of the certificates in a request may include optional extensions.	I	[RFC 2560: 2.2, DoD SPEC: 5]
One of the following definitive response indicators is used in the certificate status value: 1. good - indicates that the certificate is not revoked 2. revoked - indicates that the certificate has been revoked (either permanantly or temporarily (on hold)) 3. unknown - indicates that the responder doesn't know about the certificate being requested.	M	[RFC 2560: 2.2, DoD SPEC: 5
OCSP Responder error messages are not digitally signed.	M	[RFC 2560: 2.3]
Errors can be of the following types: 1. malformedRequest - if the request received does not conform to the OCSP syntax 2. internalError - indicates that the OCSP responder reached an inconsistent internal state 3. tryLater - indicates that the service exists, but is temporarily unable to respond 4. sigRequired - indicates that the requestor did not sign the request 5. unauthorized - the requestor is not authorized to make this query to this server	I	[RFC 2560: 2.3]
Responses can contain three times in them: 1. thisUpdate - the time at which the status being indicated was known to be correct 2. nextUpdate - the time at or before which newer information will be available about the status of the certificate 3. producedAt - the time at which the OCSP responder signed this response.	I	[RFC 2560: 2.4]
If nextUpdate is not set, the responder must have newer revocation information available all the time.	m	[RFC 2560: 2.4, 4.2.2.1]
The validity interval defined by thisUpdate and nextUpdate must correspond to the interval in CRLs.	m	[RFC 2560: 4.2.2.1]
For signature calculation, the data to be signed is encoded using the ASN.1] distinguished encoding rules (DER) [X.690].	M	[RFC 2560: 4]
Formatting of the response message could vary depending on the transport mechanism used (HTTP, SMTP, LDAP, etc.).	I	[RFC 2560: 4.2, 5]

Protocol Action	Status	Notes
The response message is formatted for HTTP.	I	Implementers are advised to consider the reliability of HTTP cache mechanisms when deploying OCSP over HTTP. [RFC 2560: 4.2, 5]
The response message is formatted for SMTP.	No	[RFC 2560: 4.2, 5]
The response message is formatted for LDAP.	I	[RFC 2560: 4.2, 5]
An OCSP response at a minimum consists of a responseStatus field indicating the processing status of the prior request.	M	[RFC 2560: 4.2.1]
If responseStatus is one of the error conditions, responseBytes are not set.	M	[RFC 2560: 4.2.1]
The value for response shall be the DER encoding of BasicOCSPResponse.	M	[RFC 2560: 4.2.1]
The value for BasicOCSPResponse signature shall be computed on the hash of the DER encoding ResponseData.	M	[RFC 2560: 4.2.1]
The CRL Entry Extensions are supported as singleExtensions.	M	[RFC2459: 5.3; RFC 2560: 4.4.5]

Status Notation:

M = Mandatory in all implementations
m = Mandatory if an option is exercised
O = Optional
O/R = Optional but recommended
o = Optional if an option is exercised
o/r = Optional if an option is exercised but recommended
I = Implemented option
NO, No = Option not used in this implementation
N/A = Does not apply to this implementation

Message Syntax

Message Field	Value	Comment
OCSPRequest	SEQUENCE	
tbsRequest		
TBSRequest	SEQUENCE	
version [0]	EXPLICIT	DEFAULT v1.
Version	00	v1(0)
requestorName [1]	EXPLICIT	
GeneralName	CHOICE	[RFC 2459: A.2]
directoryName [4]		
Name	CHOICE	Only one possibility for now. [RFC 2459: A.1]
rdnSequence		
RDNSequence	SEQUENCE OF	
RelativeDistinguishedName	SET SIZE (1 .. MAX) OF	
AttributeTypeAndValue		Arc for standard naming attributes id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
type		
AttributeType	OBJECT IDENTIFIER	
X520countryName	2.5.4.6	id-at-countryName, IS 3166 codes, PrintableString (SIZE (2))
X520CommonName	2.5.4.3	id-at-commonName
X520OrganizationName	2.5.4.10	id-at-organizationName
X520OrganizationalUnitName	2.5.4.11	id-at-organizationalUnitName
value		
AttributeValue	ANY DEFINED BY AttributeType	
DirectoryString	CHOICE	
printableString	X.500 DN: cn=(1), ou=PKI, ou=DoD, o=U.S. Government, c=US	(SIZE (1..ub-name)), (1) - varies depending on requestor [DoD SPEC: 2]
utf8String	UTF8String	(SIZE (1..ub-name)), DoD will migrate with commercial practice to UTF8
requestList	SEQUENCE OF	
Request	SEQUENCE	
reqCert		
CertID	SEQUENCE	

Message Field	Value	Comment
hashAlgorithm		[RFC 2560: 4.1.1]
AlgorithmIdentifier	SEQUENCE	[RFC 2459: 4.1.1.2, A.1]
algorithm	1.3.14.3.2.26	SHA-1 [FIPS 180-1]
parameters	NULL	ANY DEFINED BY algorithm.
issuerNameHash	OCTET STRING	Hash calculated over the DER encoding of the issuer's name field in the certificate being checked. [RFC 2560: 4.1.1, 4.1.2]
issuerKeyHash	OCTET STRING	Hash calculated over the value (excluding tag and length) of the subject public key field in the issuer's certificate. [RFC 2560: 4.1.1, 4.1.2]
serialNumber		The serial number of the certificate for which status is being requested. [RFC 2560: 4.1.1]
CertificateSerialNumber	INTEGER	[RFC 2459: 4.1, 4.1.2.2]
singleRequestExtensions [0]	EXPLICIT	
Extensions	SEQUENCE SIZE (1..MAX) OF	[RFC 2459: 4.1, 4.1.2.9, A.1]
Extension	SEQUENCE	
extnID	1.3.6.1.5.5.7.48.1.7	id-pkix-ocsp-service-locator
critical	FALSE	
extnValue	OCTET STRING	
ServiceLocator	SEQUENCE	[RFC 2560: 4.4.6]
issuer	Name	See above.
locator		
AuthorityInfoAccessSyntax	SEQUENCE SIZE (1..MAX) OF	Only certificates that can be checked by OCSP can have this extension. id-pe-authorityInfoAccess OID ::= { id-pe 1 } [RFC 2560: 3.1, RFC 2459: 4.2.2.1, A.2, B.1, DoD SPEC: 5]
AccessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp [RFC 2560: 4.4.6, RFC 2459: 4.2.2.1, DoD SPEC: 5]
accessLocation	GeneralName	http://ocsp-1.chamb.disa.mil http://ocsp-2.den.disa.mil [RFC 2560: 4.4.6, RFC 2459: 4.2.2.1, A.2, DoD SPEC: 5]

Message Field	Value	Comment
requestExtensions [2]	EXPLICIT Extensions	
AcceptableResponses	1.3.6.1.5.5.7.3.9 1.3.6.1.5.5.7.48.1 1.3.6.1.5.5.7.48.1.1 1.3.6.1.5.5.7.48.1.3 1.3.6.1.5.5.7.48.1.4 1.3.6.1.5.5.7.48.1.6 1.3.6.1.5.5.7.48.1.7	id-kp-OCSPSigning id-pkix-ocsp id-pkix-ocsp-basic id-pkix-ocsp-crl id-pkix-ocsp-response id-pkix-ocsp-archive-cutoff id-pkix-ocsp-service-locator

OCSPResponse	SEQUENCE	
responseStatus		[RFC 2560: 4.2.1]
OCSPResponseStatus	ENUMERATED	(4) is not used. [RFC 2560: 2.3]
successful (0)		Response has valid confirmations
malformedRequest (1)		Illegal confirmation request
internalError (2)		Internal error in issuer
tryLater (3)		Try again later
sigRequired (5)		Must sign the request
unauthorized (6)		Request unauthorized
responseBytes [0]	EXPLICIT	If the value of responseStatus is one of the error conditions, responseBytes are not set. [RFC 2560: 4.2.1]
ResponseBytes	SEQUENCE	
responseType	1.3.6.1.5.5.7.48.1 1.3.6.1.5.5.7.48.1.1	Must support: id-pkix-ocsp id-pkix-ocsp-basic
response	OCTET STRING	The DER encoding of BasicOCSPResponse.

BasicOCSPResponse	SEQUENCE	
tbsResponseData		
ResponseData	SEQUENCE	
version [0]	EXPLICIT Version	DEFAULT v1.
responderID		
ResponderID	CHOICE	
byName [1]	Name	
byKey [2]		The key used to sign the response MUST belong to the CA who issued the certificate in question [RFC 2560: 2.2]

Message Field	Value	Comment
KeyHash	OCTET STRING	SHA-1 hash of responder's public key (excluding the tag and length fields).
producedAt		The time at which the OCSP responder signed this response. [RFC 2560: 2.4]
GeneralizedTime	YYYYMMDDHHMMSSZ	[RFC 2459: 4.1.2.5.2]
responses	SEQUENCE OF	
SingleResponse	SEQUENCE	
certID	CertID	The certificate for which status is being provided.
certStatus		
CertStatus	CHOICE	
good [0]	IMPLICIT NULL	A positive response indicating that the certificate is not revoked. Does not necessarily mean that the certificate was ever issued, or that at the response time the certificate was still valid. Response extensions may be used to convey additional information [RFC 2560: 2.2]
revoked [1]	IMPLICIT	The certificate has been revoked (either permanantly or temporarily (on hold)). [RFC 2560: 2.2]
RevokedInfo	SEQUENCE	
revocationTime	GeneralizedTime	
revocationReason [0]	EXPLICIT	
CRLReason	ENUMERATED	[X.509: 12.5.2.2, DoD SPEC: 3]
keyCompromise (1)		
cACompromise (2)		Responder MAY return revoked state for all certificates issued by a compromised CA. [RFC 2560: 2.7]
affiliationChanged (3)		
superseded (4)		
cessationOfOperation (5)		
unknown [2]	IMPLICIT	Indicates that the responder doesn't know about the certificate being requested. [RFC 2560: 2.2]
UnknownInfo	NULL	This can be replaced with an enumeration.
thisUpdate	GeneralizedTime	The time at which the status being indicated is known to be correct. [RFC 2560: 2.4]
nextUpdate [0]	EXPLICIT GeneralizedTime	The time at or before which newer information will be available about the status of the certificate. [RFC 2560: 2.4]
singleExtensions [1]	EXPLICIT Extensions	

Message Field	Value	Comment
CrlID	SEQUENCE	id-pkix-ocsp-crl OID ::= { id-pkix-ocsp 3 } [RFC 2560: 4.4.2]
crlUrl [0]	EXPLICIT IA5String	The URL at which the CRL is available.
ArchiveCutoff	GeneralizedTime	id-pkix-ocsp-archive-cutoff OID ::= { id-pkix-ocsp 6 } [RFC 2560: 4.4.4]
CRLReason	ENUMERATED	id-ce-cRLReason OID ::= { id-ce 21 } [RFC 2459: 5.3.1]
invalidityDate	GeneralizedTime	ZULU Time id-ce-invalidityDate OID ::= { id-ce 24 } [RFC 2459: 5.3.3]
Signature	SEQUENCE	
signatureAlgorithm		[RFC 2560:4.3; RFC 2459: 7.2.1, 7.2.2, DoD SPEC: 2]
AlgorithmIdentifier	SEQUENCE	[RFC 2459: 4.1.1.2, A.1]
algorithm	1.2.840.113549.1.1.5	sha1With RSAEncryption [RFC 2437]
parameters	NULL	ANY DEFINED BY algorithm. [RFC 2459: 7.2.1]
signature	BIT STRING	The value for signature shall be computed on the hash of the DER encoding ResponseData. [RFC 2560: 2.2, 4.2.1]

Digitally signed by Gregor D. Scott
cn=Gregor D. Scott, ou=JIEO-JEBBB, o=Defense Information Systems Agency, c=US
Date: 2000.05.23 16:54:49 -05'00'
Reason: I am approving this document
Ft. Monmouth, NJ 07703-5613